Docket No.: 2454.1043

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Steffen FRIES

Serial No. 10/580,954 Group Art Unit: 2437

Confirmation No. 8341

Filed: May 30, 2006 Examiner: Jeffrey L. Williams

For: SECURITY MODULE FOR ENCRYPTING A TELEPHONE CONVERSATION

APPEAL BRIEF UNDER 37 C.F.R § 41.37

Mail Stop Appeal Brief-Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In a Notice of Appeal filed June 24, 2011, the Applicant appealed the Examiner's March 29, 2011 Office Action finally rejecting claims 11, 14-15, 17, 20-21, and 23. Appellants' Brief, together with the requisite fee set forth in 37 C.F.R. § 1.17, is submitted herewith.

The due date for filing this Appeal Brief was two months from the June 24, 2011 filing date of the Notice of Appeal. Therefore, this Appeal Brief is being filed on September 26, 2011 with a Petition for a one-month extension of time (September 24-25, 2011 being a Saturday and Sunday).

Should any additional fees be required or an overpayment of fees made, please debit or credit our Deposit Account No. 19-3935, as needed.

09/27/2011 SZEWDIE1 00000001 10580954
02 FC:1402 620.00 OP

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest is Siemens Aktiengesellschaft, the assignee of the application.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

Appellant, appellant's legal representative, and the assignee do not know of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

Claims 11, 14-15, 17, 20-21, and 23 have been finally rejected and are on appeal.

Claims 1-10, 12-13, 16, 18-19, and 22 have been cancelled.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

Appellants' most recent Response filed March 7, 2011 was entered for purposes of Appeal as indicated by the Office Action mailed March 29, 2011.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

Independent claim 11 recites a security module (for example, see security module SM in the figure) for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network (for example, see VoIP clients VoIP-C on the local area network LAN in the figure), and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network (for example, see TDM clients TDM-C on the public TDM telephone network in the figure) and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway (for example, see gateway G in the figure and paragraph [0015], wherein the TDM network is a digital network, with a special analog speech channel being used however for transmission of spoken words, the LAN and the TDM network are connected to each other via gateway G, and the gateway is used to modify IP data packets transmitted in the LAN network for forwarding in the TDM network as well as data from the TDM network for forwarding in the LAN network in the appropriate manner). The claimed security module is connected into a connecting line of one of the first and second telecommunication terminals (for example, see the figure) and includes a protocol processing unit processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which the security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at the security module after transport via the encrypted transport protocol, into voice signals (for example, see paragraph [0019] and the double arrows MIKEY-KM and STRP-MS in the figure). The claimed security module further includes a modem connection unit, used when the security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection (for example, see paragraphs [0020]-[0022]). Furthermore, a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol (for example, see paragraphs [0020]-[0022] and double arrow IP-PPP-TDM in the figure). Furthermore, the

encrypted transport protocol is Secure Real Time Transport Protocol (for example, see paragraphs [0019]-[0022]).

Independent claim 23 recites a method performed by a security module (for example, see security module SM in the figure) for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network (for example, see VoIP clients VoIP-C on the local area network LAN in the figure) and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network (for example, see TDM clients TDM-C on the public TDM telephone network in the figure) and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway (for example, see gateway G in the figure and paragraph [0015], wherein the TDM network is a digital network, with a special analog speech channel being used however for transmission of spoken words, the LAN and the TDM network are connected to each other via gateway G, and the gateway is used to modify IP data packets transmitted in the LAN network for forwarding in the TDM network as well as data from the TDM network for forwarding in the LAN network in the appropriate manner), wherein the security module is connected into a connecting line of one of the first and second telecommunication terminals (for example, see the figure). The claimed method includes processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which the security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at the security module after transport via the encrypted transport protocol, into voice signals (for example, see paragraph [0019] and the double arrows MIKEY-KM and STRP-MS in the figure). The claimed method further includes when the security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection (for example, see paragraphs [0020]-[0022]). The claimed method further includes using a point-to-point protocol connection over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange

protocol (for example, see paragraphs [0020]-[0022] and double arrow IP-PPP-TDM in the figure). Furthermore, the encrypted transport protocol is Secure Real Time Transport Protocol (for example, see paragraphs [0019]-[0022]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

The specification stands objected to as failing to provide proper antecedent basis for the claimed subject matter.

Claims 11, 14-15, 17, 20-21, and 23 stand rejected under the first paragraph of 35 USC § 112 as failing to comply with the written description requirement.

Claims 11, 14-15, 17, 20-21, and 23 stand rejected under the second paragraph of 35 USC § 112 as being indefinite.

Claims 11, 14-15, 17, 20-21, and 23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0009659 to DiSanto et al. (hereinafter "DiSanto") in view of the article "*Conversational IP multimedia Security*" by Blom et al. (hereinafter "Blom").

VII. ARGUMENT

A. Review of the prior art

1. U.S. Patent Application Publication No. 2003/0009659 ("DiSanto ")

DiSanto discloses a portable security device for providing secure communications over a plurality of networks is presented. In one embodiment, the device comprises, at least one communication port for transfer of audio data, at least one communication port for transfer of digital data, a keypad, an encoding/decoding device, a conversion device operable to covert between audio and digital data and a processor, in communication with a memory, the keypad, the encoding/decoding device, operable to execute code for selecting a configuration of a transmission and a reception port from among the communication ports dependent upon the presence of a network communication device and an input/output device in communication with the selected ports, providing data received from the selected reception port to the encryption/decryption device for encrypting; and providing said encrypted data to the selected transmission port. In one aspect of the invention, encrypted voice data can be transferred over a wireless network using cellular phones, over a wired and wireless network using land-based telephones, cellular phones or satellite phones. In another aspect, encrypted computer data may be transferred over wired or wireless networks.

2. Conversational IP multimedia Security ("Blom")

Blom discloses the security requirements that emerge from conversational IP multimedia applications in heterogeneous environments, with special emphasis on the requirements stemming from the wireless access. The design and the design goals of both SRTP, a security protocol for protection of media traffic, and multimedia Internet keying (MIKEY), a key management protocol specially developed for those environments, are also described.

B. The specification provides proper antecedent basis for the claimed subject matter

In the Final Office Action, the Examiner objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

This objection to the specification is respectfully traversed and withdrawal is respectfully requested.

More specifically, the Examiner has objected to the claim limitation "a public switched telephone network that is distinct from the packet-oriented data network." The Examiner appears to take the position that this feature is not supported in the specification because it is disclosed that the public switched telephone network can be an ISDN. However, this is irrelevant to whether or not the claimed public switched telephone network is distinct from the claimed packet-oriented data network. In other words, just because a public switched telephone network can be an ISDN, it does not follow that the disclosure does not support the position that there are two distinct networks, one being a public switched telephone network and the other being a packet-oriented data network in at least one embodiment. Fig. 1 of the drawings and the corresponding disclosure clearly indicate that there is both an IP-based LAN and a separate and distinct public TDM telephone network. For example, paragraph [0015] of the specification clearly states "the **heterogeneous network** shown in Figure 1 on the one hand includes an IP-based LAN (LAN = Local Area Network) **as well as** a public TDM (TDM = Time Division Multiplexing) telephone network."

To begin with, one of ordinary skill in the art would clearly appreciate that the term heterogeneous network refers to network in which devices with different protocols are connected. As such, based on the disclosure in the specification, one of ordinary skill in the art would clearly appreciate that the claimed public switched telephone network is distinct from the claimed packet-oriented data network. Furthermore, the figure of the drawings clearly illustrates that the IP-based LAN is separate and distinct from the public TDM telephone network and that the two are separated by the gateway G.

C. Claims 11, 14-15, 17, 20-21, and 23 comply with the written description requirement

In the Final Office Action, the Examiner rejected claims 11, 14-15, 17, 20-21, and 23 under the first paragraph of 35 USC § 112 as failing to comply with the written description requirement.

This rejection is respectfully traversed and withdrawal is respectfully requested.

For the reasons discussed above with respect to the objection to the specification, it is submitted that claims 11, 14-15, 17, 20-21, and 23 do comply with the written description requirement with respect to the claimed feature of "a public switched telephone network that is distinct from the packet-oriented data network."

The figure of the drawings and the corresponding disclosure clearly indicate that there is both an IP-based LAN and a separate and distinct public TDM telephone network. For example, paragraph [0015] of the specification clearly states "the **heterogeneous network** shown in Figure 1 on the one hand includes an IP-based LAN (LAN = Local Area Network) **as well as** a public TDM (TDM = Time Division Multiplexing) telephone network."

To begin with, one of ordinary skill in the art would clearly appreciate that the term heterogeneous network refers to network in which devices with different protocols are connected. As such, based on the disclosure in the specification, one of ordinary skill in the art would clearly appreciate that the claimed public switched telephone network is distinct from the claimed packet-oriented data network. Furthermore, the figure of the drawings clearly illustrates that the IP-based LAN is separate and distinct from the public TDM telephone network and that the two are separated by the gateway G.

D. Claims 11, 14-15, 17, 20-21, and 23 are definite

In the Final Office Action, the Examiner rejected claims 11, 14-15, 17, 20-21, and 23 under the second paragraph of 35 USC § 112 as being indefinite.

This rejection is respectfully traversed and withdrawal is respectfully requested.

For the reasons discussed above with respect to the objection to the specification, it is submitted that claims 11, 14-15, 17, 20-21, and 23 are definite with respect to the claimed feature of "a public switched telephone network that is distinct from the packet-oriented data network."

The figure of the drawings and the corresponding disclosure clearly indicate that there is both an IP-based LAN and a separate and distinct public TDM telephone network. For example, paragraph [0015] of the specification clearly states "the **heterogeneous network** shown in Figure 1 on the one hand includes an IP-based LAN (LAN = Local Area Network) **as well as** a public TDM (TDM = Time Division Multiplexing) telephone network."

To begin with, one of ordinary skill in the art would clearly appreciate that the term heterogeneous network refers to network in which devices with different protocols are connected. As such, based on the disclosure in the specification, one of ordinary skill in the art would clearly appreciate that the claimed public switched telephone network is distinct from the claimed packet-oriented data network. Furthermore, the figure of the drawings clearly illustrates

that the IP-based LAN is separate and distinct from the public TDM telephone network and that the two are separated by the gateway G.

E. Claims 11, 14-15, 17, 20-21, and 23 are patentable over the combination of DiSanto and Blom

In the Final Office Action, claims 11, 14-15, 17, 20-21, and 23 were rejected under 35 U.S.C. §103(a) as being unpatentable over DiSanto in view Blom.

It is submitted that the Examiner failed to establish a prima facie case of obviousness. The references to DiSanto in view Blom, alone or in combination, do not teach or suggest or make obvious all the features of claims 11, 14-15, 17, 20-21, and 23.

Independent claim 11 recites:

> A security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising
>
> a protocol processing unit processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;
>
> a modem connection unit, used when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection, wherein
>
> a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange

protocol, and

the encrypted transport protocol is Secure Real Time Transport Protocol.

As such, claim 11 provides a protocol processing unit that processes data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol. Furthermore, claim 11 includes a modem connection unit, used when the security module is connected in a connecting line at a second telecommunication terminal, that transports the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the security module of claim 11 provides for end-to-end encryption between a client in a packet-oriented network and a client in a public switched telephone network (analog or digital), which is distinct from the packet-oriented network, using the key exchange protocol and the encrypted transport protocol (SRTP) because each of the two distinct networks distinctly use the key exchange protocol and the encrypted transport protocol via the claimed protocol processing unit and modem connection unit, respectively. These features are not taught by either DiSanto or Blom.

The Examiner's statement that applicant is arguing that the claimed networks "use" the recited key exchange protocol and the encrypted transport protocol is not correct. As clearly stated, applicant is asserting that each of the recited key exchange protocol and the encrypted transport protocol are provided via the claimed protocol processing unit and modem connection unit, which are part of the claimed security module.

Furthermore, the modem of DiSanto does not correspond to the claimed modem connection unit, as indicated by the Examiner. As discussed above, the claimed modem connection unit is used when the security module is connected in a connecting line at a second PSTN telecommunication terminal for transporting the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the claimed modem connection unit provides a transfer of encrypted communications from the packet-oriented network into the PSTN because the packet-oriented network also uses the encrypted transport protocol with keys for the encrypted transport protocol exchanged using the key exchange protocol.

DiSanto merely discloses a security device for secure communication over a plurality of networks (see the Abstract of DiSanto). The internal modem 240 in FIG. 2B of DiSanto is used to perform analog to digital conversion when digitized voice data is directed to port 245 (see paragraph [0033] of DiSanto). Thus, the modem 240 is used merely to comply with the technical requirements of a respective network, but does not provide a technical solution enabling encryption of voice data in a heterogeneous network including a packet-oriented network and a PSTN. Again, DiSanto does not disclose a heterogeneous network including a separate and distinct packet-oriented network and PSTN. Thus, it follows that the internal modem 240 of DiSanto cannot perform the function as providing a path for encrypted communication as stated by the Examiner and as recited in independent claim 11.

Furthermore, claim 11 specifies that "a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol." The Examiner alleges that this feature is anticipated by "a procedure for establishing a direct connection between two nodes" disclosed in DiSanto. However, unlike in DiSanto, the modem of the claimed security module enables the data packets from the packet-oriented network to be transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. The procedure for establishing a direct connection between two nodes in DiSanto does not anticipate or render obvious this type of connection among terminals of different networks.

It is respectfully submitted that the Examiner must consider the limitation. As is clear from MPEP §2173.05(g), there is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. In re Swinehart, 439 F.2d 210, 169 USPQ 226 (CCPA 1971). "A functional limitation must be evaluated and considered, just like any other limitation of the claim, for what it fairly conveys to a person of ordinary skill in the pertinent art in the context in which it is used," e.g., a functional limitation may be used to functionally define a particular capability or purpose that is served by the recited element.

In asserting an intended use argument, the prior art structure must be capable of performing the intended use. See, e.g., *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997). Thus, DiSanto must be enabled to accomplish the claimed functional language of the present invention as set forth in claim 11, for example. Specifically,

DiSanto must be enabled to include:

> processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals; and
>
> setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection.

Blom has been cited by the Examiner merely as an example of the use of the Secure Real Time Transport Protocol and otherwise fails to make up for the deficiencies in DiSanto discussed above with respect to independent claim 11.

Thus, for at least for the reasons discussed, it is respectfully submitted that claim 11, and claims 14-15, 17, and 20-21 depending from claim 11, patentably distinguish over the combination of DiSanto and Blom.

Independent claim 23 recites:

> A method performed by a security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising
>
> processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving

at said security module after transport via the encrypted transport protocol, into voice signals;

when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection; and

using a point-to-point protocol connection over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, wherein

the encrypted transport protocol is Secure Real Time Transport Protocol.

For at least the reasons discussed above with respect to claim 11, it is respectfully submitted that the combination of DiSanto and Blom does not teach or make obvious each of the features of claim 23, so that claim 23 patentably distinguishes over the combination of DiSanto and Blom.

F. CONCLUSION

In summary, Applicant submits that claims 11, 14-15, 17, 20-21, and 23 patentably distinguish over the prior art.

Reversal of the Examiner's rejections is respectfully requested.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 9-26-11

By: _____

Aaron C. Walker

Registration No. 59,921

VIII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

1-10. (Cancelled)

11. (Previously Presented) A security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising:

a protocol processing unit processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;

a modem connection unit, used when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection, wherein

a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, and

the encrypted transport protocol is Secure Real Time Transport Protocol.

12-13. (Cancelled)

14. (Previously Presented) A security module in accordance with claim 11, wherein the key exchange protocol is multimedia Internet keying.

15. (Previously Presented) A security module in accordance with claim 11, wherein for a telephone conversation, messages of the key exchange protocol are transported via a session initiation protocol, and

wherein said protocol processing unit processes the session initiation protocol.

16. (Cancelled)

17. (Previously Presented) A security module in accordance with claim 11, wherein the telephone network is an ISDN network, and said modem connection unit sets up the modem connection over a B-channel in the ISDN network.

18-19. (Cancelled)

20. (Previously Presented) A security module in accordance with claim 11, wherein the packet-oriented network is an Internet protocol-based data network and a local area network, and said modem connection unit sets up the modem connection in accordance with at least one of a V90 and a V92 standard.

21. (Previously Presented) A security module in accordance with claim 20, wherein said security module is connected into a connecting cable between a telephone handset and the one of the first and second telecommunication terminals.

22. (Cancelled)

23. (Previously Presented) A method performed by a security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented

network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising:

processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;

when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection; and

using a point-to-point protocol connection over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, wherein

the encrypted transport protocol is Secure Real Time Transport Protocol.

IX. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

Not applicable

X. RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Not applicable